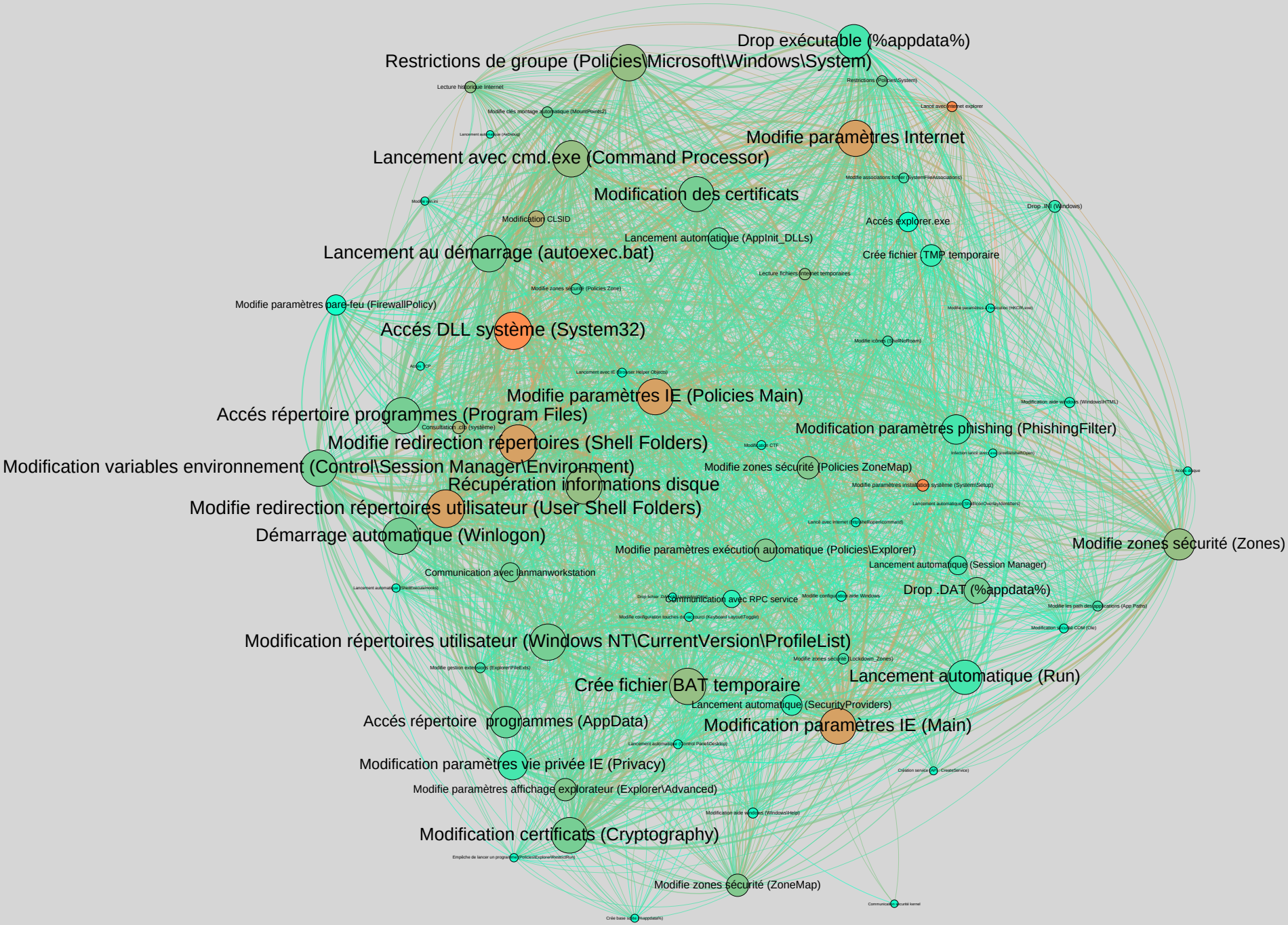
Drop exécutable (%appdata%)
Restrictions de groupe (Policies\Microsoft\Windows\System)
Lecture historique Internet
Modifie clés montage automatique (MountPoints2)
Modifie paramètres Internet
Lancement avec cmd.exe (Command Processor)
Modification des certificats
Modification CLSID
Accés explorer.exe
Lancement automatique (AppInit_DLLs)
Lancement au démarrage (autoexec.bat)
Crée fichier .TMP temporaire
Lecture fichiers Internet temporaires
Modifie zones sécurité (Policies Zone)
Modifie paramètres pare-feu (FirewallPolicy)
Accés DLL système (System32)
Modifie paramètres IE (Policies Main)
Accés répertoire programmes (Program Files)
Consultation .clb (système)
Modification paramètres phishing (PhishingFilter)
Modifie redirection répertoires (Shell Folders)
Modification variables environnement (Control\Session Manager\Environment)
Modifie zones sécurité (Policies ZoneMap)
Récupération informations disque
Modifie redirection répertoires utilisateur (User Shell Folders)
Démarrage automatique (Winlogon)
Modifie zones sécurité (Zones)
Modifie paramètres exécution automatique (Policies\Explorer)
Lancement automatique (Session Manager)
Communication avec lanmanworkstation
Drop .DAT (%appdata%)
Communication avec RPC service
Modification répertoires utilisateur (Windows NT\CurrentVersion\ProfileList)
Lancement automatique (Run)
Crée fichier BAT temporaire
Lancement automatique (SecurityProviders)
Accés répertoire programmes (AppData)
Modification paramètres IE (Main)
Modification paramètres vie privée IE (Privacy)
Modifie paramètres affichage explorateur (Explorer\Advanced)
Modification certificats (Cryptography)
Modifie zones sécurité (ZoneMap)